JUDGE BENJAMIN H. SETTLE

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, vs. DAVID MICHAEL NAVARRO, Defendant.	NO. CR13-5525BHS OPPOSITION TO GOVERNMENT'S APPLICATION FOR AN ORDER TO DIRECT APPLE TO UNLOCK AN iPHONE

A. The Government Must Give Apple an Opportunity to Be Heard on the Government's Application, If it Has Not Already Done So.

Mr. Navarro's Memorandum in Opposition to ex Parte Proceeding (Dkt. 34) discussed the Ninth Circuit's decision in *United States v. Mountain States Tel. & Tel. Co.*, 616 F.2d 1122 (9th Cir. 1980). The court held that in the case of Government applications such as this one, the third party (in this case Apple) "should be afforded reasonable notice and an opportunity to be heard prior to the entry of any order compelling its assistance." *Id*. at 1133. *Accord*, *Application of U. S. of Am. for Order Authorizing Installation of Pen Register or Touch-Tone Decoder & Terminating Trap*, 610 F.2d 1148, 1157 (3d Cir. 1979) ("We conclude that due process requires a hearing on the issue of burdensomeness before compelling a telephone company to provide tracing assistance").

The Government's Application and supporting papers do not reflect that Apple was given notice that an Application would be filed, such that it had an opportunity to be heard. It

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

reflects that "[a] representative of Apple has already reviewed an unsigned copy of the proposed order presented with the government's application in this matter, and has indicated to me that, when presented with a signed copy of the order, Apple" would comply with the order. Declaration of Counsel in Support of Government's ex Parte Application for an Order to Direct Apple to Unlock an iPhone at 3.

Thus, Apple knew of the potential that the Government would obtain such an order. However, the Government's Application does not reflect that Apple knew that it would have "an opportunity to be heard prior to the entry of any order compelling its assistance." Simply informing a party that one might obtain a court order is not comparable to informing the party that it has the right to be heard on the matter, or when or where that opportunity might occur.

Despite the lack of evidence in the record, Apple may have been given such notice, in which case the Government has complied with its obligations under *Mountain States*. But if Apple has not been given the required notice, it should be afforded that notice before this Court issues any order.

B. The Factual Basis for the Application is Missing.

Much of the factual support for the Application consists of vague representations of Government counsel. Both the Application itself and the accompanying Declaration refer to the statements of unnamed Government counsel in unidentified districts and to the orders issued by unidentified courts in unidentified cases. The Application even makes factual assertions that lack any support in the Declaration of counsel, most notably the assertion that "the order is not likely to place any unreasonable burden on Apple." Application at 3.

Mr. Navarro leaves to the Court's discretion where this factual showing is adequate to obtain an order, and focuses his argument on the scope of any order that this Court might issue.

//

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

C. The Court Should Impose Restrictions on the Government's Access to the Cell Phone Consistent With the Ninth Circuit's Admonitions in *Comprehensive Drug Testing*.

For purposes of responding to the Government's Application, Mr. Navarro will assume that this Court has authority to issue the requested order, once Apple has been given notice and once there is adequate factual support for the Application.[1] However, there is a significant question regarding the terms of any order that this Court may issue.

D. Giving the Government Access to All the Data on Mr. Navarro's Cell Phone, Rather than Just the Data Within the Scope of the Warrant, Threatens His Privacy Interests.

Mr. Navarro starts with two basic principles. He has no right to interfere with the Government's ability to examine all items for which it has a valid warrant based on probable cause to believe that they come within the reach of a proper search warrant. On the other hand, the Government has no right to view Mr. Navarro's private data that is outside the scope of a proper search warrant, unless truly necessary in order to view the data that is within that scope.[2] Mr. Navarro may have the most private of material stored on his cell phone that has nothing to do with the Government's investigation, and the Government should not be allowed to view that material.

So-called "smartphones" like the iPhone at issue here are sufficiently ubiquitous that this Court hardly needs reminding of their powerful data-storage capabilities. "Smartphones are no more than small computers that happen to make phone calls." Sharon D. Nelson, John W. Simek, *Top 16 Security Tips for Smartphones*, 86 Wisconsin Lawyer 43 (April 2013). They therefore are "extremely powerful devices, capable of storing contacts, calendar entries, email communications, electronic files, voice messages, and a host of additional confidential

---

[1] For this reason, Mr. Navarro's proposed order does not address the question of whether the order to Apple should issue but instead addresses the conditions that should apply to any such order.

[2] For purposes of this Opposition, Mr. Navarro will assume that the phone is his.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

[] information." *Id*. *Accord, United States v. Gomez*, 807 F. Supp. 2d 1134, 1138 (S.D. Fla. 2011) (describing an iPhone as "maintaining sophisticated computer-like data storage capabilities").

As a result, regardless of whether the cell phone contains data within the scope of the search warrant, it may well contain a huge quantity of data outside the scope of the search warrant, revealing the most intimate aspects of Mr. Navarro's private and lawful life. The Government is entitled to everything within the scope of a valid search warrant; however, it is not entitled to any of the latter category. Thus, the search of the cell phone in this case presents the issue of intermingled data, a problem occurring with increasing frequency in this era of searches of computers and computer-like devices.

The Ninth Circuit spoke to problem of intermingled data in *United States v. Tamura*, 694 F.2d 591 (9th Cir.1982); it again focused on that problem, this time in the context of electronic data, in *United States v. Comprehensive Drug Testing*, Inc., 621 F.3d 1162 (9th Cir. 2010) (en banc). The *CDT* began by discussing the problem faced by law enforcement:

> There is no way to be sure exactly what an electronic file contains without somehow examining its contents—either by opening it and looking, using specialized forensic software, keyword searching or some other such technique. But electronic files are generally found on media that also contain thousands or millions of other files among which the sought-after data may be stored or concealed. By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.

Id. at 1176.

But this problem for law enforcement also creates a problem for the privacy interests of the individual (and therefore for society at large): "Authorization to search some computer files therefore automatically becomes authorization to search all files in the same subdirectory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media." *Id*. at 1176. As a result, the needs of law enforcement "create[] a serious risk

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.*

The court discussed the Government's approach to the two competing interests, which was to completely ignore the privacy interests. "Let's take everything back to the lab, have a good look around and see what we might stumble upon." *Id*. at 1171. The court warned that this approach "would make a mockery of *Tamura* . . ." *Id.*

The court stated that "[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id*. at 1177. Without requiring any specific methodology, the court concluded that "[t]his calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *Id*.

The concurrence suggested some particular means to accomplish that goal. These include requiring the Government to "waive reliance upon the plain view doctrine in digital evidence cases." *Id*. at 1180. Other means include the use of taint teams and requiring that "[t]he government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents." *Id*. (The court's opinion in CDT reflects that one of the warrants at issue had included a requirement that only computer experts, and not the investigative agent, view the seized files. 621 F.3d at 1173.)

The proposed order includes the plain view waiver, as well as the other two methods (although giving the Government the flexibility to choose one of those latter two methods as alternatives), using language borrowed closely from the concurrence. If this Court had concerns about requiring a waiver of plain view, requiring the choice of the other two methods would still go far towards satisfying Mr. Navarro's concerns.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

E. The search warrant Does Not Contain Adequate Protections Consistent with CDT's Admonitions.

The Government may contend that the search warrant in fact adequately protects Mr. Navarro's privacy interests, i.e. that it ensures that the Government will examine only material within the scope of the warrant. Although the search warrant application contains language that appears to provide such assurances, those assurances are illusory.

For example, the affidavit "anticipates the use of a hash value library to exclude normal operating system files that do not need to be searched[.]" Affidavit at 8. Even putting aside the non-committal nature of the word "anticipates," the issue is far less the Government's review of operating system files than of documents, email, diaries, and similar personal items, if they are outside the scope of the warrant.

Similarly, the affidavit "anticipates the use of hash values and known file filters to assist the digital forensics examiners/agents in identifying known and/or suspected child pornography image files. Use of these tools will allow for the quick identification of evidentiary files but also assist in the filtering of normal system files that would have no bearing on the case." *Id.* This passage, too, does not commit to allowing agents to view only files that come within the scope of the warrant.

In another passage, the affidavit states that "the search. techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant" the warrant. *Id.* This might seem to justify some comfort about the scope of the search, except for two things. First, this passage talks of techniques reasonably expected to find items within the warrant's scope. It does not speak of excluding items outside that scope.

Lest that be thought to be nit-picking, the affidavit is quite explicit about allowing a full-scale search of all of a device's contents. The affidavit states that "law enforcement personnel may then examine all of the data contained in the forensic images and/or on the digital devices

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant." *Id.* In other words, the affidavit provides for exactly what the *CDT* opinion (and not just the concurrence) condemns: "Let's take everything back to the lab, have a good look around and see what we might stumble upon." *Id*. at 1171. The affidavit expressly envisions that *all* of the intermingled data may be examined by law enforcement, regardless of whether it comes within the scope of the warrant. This Court should not issue an order that assists the Government in viewing evidence outside the scope of the warrant.

F. It is Appropriate for this Court to Ensure that the Government's Search Properly Balances Mr. Navarro's Interests and the Government's, Notwithstanding the Existing Search Warrant.

The Government may argue that because the magistrate has issued the search warrant for the cell phone, this Court is restricted to simply approving the order to Apple to implement the dictates of the search warrant. In other words, the Government may argue, this Court should not address any of the *CDT* court's concerns – either the magistrate addressed them adequately, or it did not, but that is none of this Court's business. Should the Government make such an argument, it would be wrong.

"The All Writs Act invests a court with a power [that is] essentially equitable . . ." *Clinton v. Goldsmith*, 526 U.S. 529, 530 (1999). The Government is asking this Court to use its equitable power to require a third party to assist the Government in an endeavor. Even if that endeavor has already been approved by a magistrate, this Court should insist that, if its equitable powers are being called upon, those powers be used to properly balance the Government's legitimate law enforcement interests and Mr. Navarro's legitimate privacy interests.

As discussed in Mr. Navarro's Memorandum in Opposition to ex Parte Proceeding (Dkt. 34), his remedies to challenge the search warrant after the fact are limited. They would never actually remedy any violation of his privacy interests but would at most

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

lead to the suppression of evidence or money damages. Even if the Government acted unconstitutionally, the suppression remedy would normally be unavailable if the Government showed good faith reliance on a search warrant. Furthermore, the search warrant might not be unconstitutional but still not strike the most appropriate balance between Mr. Navarro's privacy rights and the Government's investigative needs. In that case, Mr. Navarro would have no remedy at all to protect his privacy rights.

In short, Mr. Navarro does not have an adequate remedy at law. The time to protect Mr. Navarro's legitimate privacy interests (while also protecting the Government's legitimate investigative needs) is *before* the Government examines the cell phone, not after. It is completely appropriate for this Court to reject an "all or nothing" approach but instead to use its equitable powers to strike the proper balance of interests.

The Government may also point to the recent decision in *United States v. Schesso*, --- F.3d ----, 2013 WL 5227071, at *6 (9th Cir. Sept. 18, 2013) (petition for rehearing en banc pending), which discussed *CDT* and declined to suppress evidence based on a lack of search protocols. Nothing in *Schesso* suggests that this Court should decline to issue the order the way Mr. Navarro suggests. The *Schesso* court reversed a suppression order because the only item sought to be suppressed was squarely within the scope of the warrant. *Id*. at *7. Further, in *Schesso*, there was no indication that the computer expert "disclosed to [the investigating agent] 'any information other than that which [was] the target of the warrant.'" *Id*. (quoting *CDT* at 1180. The court also concluded that "nor did [the search] expose sensitive information about Schesso other than his possession of and dealing in child pornography." *Id.*

Here, the goal is to ensure just that – preventing the search from exposing information about Mr. Navarro other than that responsive to the search warrant and keeping such material being disclosed to the investigating agents. In fact, the court specifically noted that courts

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

"may consider such protocols or a variation on those protocols as appropriate in electronic searches." *Id*. at *8. It then observed:

> Ultimately, the proper balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures of electronic data must be determined on a case-by-case basis. The more scrupulous law enforcement agents and judicial officers are in applying for and issuing warrants, the less likely it is that those warrants will end up being scrutinized by the court of appeals.

Id.

The *Schesso* court noted that the specific protocols discussed in the *CDT* concurrence were not constitutional requirements. That is irrelevant for the issue posed here - how can this Court best exercise its equitable powers to properly balance two competing interests, one being Mr. Navarro's privacy interests in the Government not viewing his data that lies outside the scope of the search warrant.

In other words, the *Schesso* decision – rejecting suppression of an item within the scope of a search warrant, when investigating agents viewed nothing outside the scope of that warrant – has nothing to say about how a court should exercise its powers prospectively to protect privacy interests and investigative interests. Given that the affidavit specifically envisions that the Government would view *all* of the device's data, and not just that within the scope of the warrant, this Court should issue an order that appropriately balances the competing interests.

CONCLUSION

If the Court decides to issue the order requested by the Government, it should include in the order requirements to ensure that the Government does not view any contents of Mr.

//

//

//

//

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

Navarro's cell phone that are outside the scope of the warrant. The Proposed Order that Mr. Navarro has filed accomplishes that goal.

DATED this 1st day of November, 2013.

Respectfully submitted,

s/ *Miriam Schwartz*
MIRIAM SCHWARTZ
Attorney for David M. Navarro

s/ *Alan Zarky*
ALAN ZARKY
Research and Writing Attorney

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on the date below I filed with the Clerk of the Court the foregoing Opposition to Government's Application for an Order to Direct Apple to Unlock an iPhone. I used the CM/ECF system, which will send notification of this filing to Assistant United States Attorney Marci Ellsworth.

DATED this 1st day of November, 2013.

s/ Delia Bonaparte

FEDERAL PUBLIC DEFENDER
1331 Broadway, Ste. 400
Tacoma, Washington 98402
(253) 593-6710